Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Secondly, suppose that α_2 is not a factor of $P-1$. Let $P^e-1\equiv 0 \pmod{\alpha_2}$, where e is the smallest exponent of P for which this congruence holds, and let P^e-1 be divisible by $\alpha_2{}^l$, but by no higher power of α_2. Then, since it is necessary that $P^a-1\equiv 0 \pmod{\alpha_2{}^b}$, if $l<b$, $P^{e\alpha_2{}^{b-l}}-1\equiv 0 \pmod{\alpha_2{}^b}$, while this is the lowest number of this form which is divisible by $\alpha_2{}^b$. Therefore, it is necessary that α should be a multiple of $e\alpha_2{}^{b-l}$, and since e must be a factor of α_2-1 by Fermat's Theorem, and is therefore relatively prime to α_2, e must be a divisor of $\alpha/\alpha_2{}^b$. It is, therefore, necessary and sufficient that α be divisible by e.

If $l>b$, P^e-1 is the lowest number of this form which is divisible by $\alpha_2{}^b$, and we have as before that the necessary and sufficient condition is that α shall be divisible by e.

It can be shown that δ and $P-1$ can have no common factor. If they had a common prime factor δ_1, then since

$$\frac{P^{\alpha}-1}{P-1}=P^{\alpha-1}+P^{\alpha-2}+\ldots+P+1\equiv+1+\ldots+1\equiv\alpha \pmod{\delta_1},$$

δ_1 must be a factor of α. Suppose that $\delta_1=\alpha_1$. Then, since the numerator $P^{\alpha}-1$ is divisible by $\alpha_1{}^{m+a}$ and by no higher power, while in the denominator α contains $\alpha_1{}^a$ and $P-1$ contains $\alpha_1{}^m$, and δ contains α, to at least the first power, then the denominator would contain $\alpha_1{}^{m+a+1}$, so the fraction could not be equal to an integer.

Theorem. *The necessary and sufficient conditions that* $(P^{\alpha}-1)/\delta\alpha(P-1)$ *shall be integral are: (1) α must be divisible by e, the least integer such that P^e-1 is divisible by α_κ, where for α_κ is taken in turn the various prime factors of α not dividing $P-1$; (2) δ is any divisor of* $(P^{\alpha}-1)/a(P-1)$.

Example. Let $P=3^6$. Then $P-1=2^3.7.13$. Let $\alpha_1=7$, $\alpha_2=23$. Then $e=11$, since $P^{11}\equiv 1 \pmod{23}$. Therefore α must be a multiple of 7, 23, and 11. For example, let $\alpha=7.11.23$. Then δ may be taken as any divisor of $\dfrac{3^{6\cdot7\cdot11\cdot23}-1}{7.11.23(3^6-1)}$; for example, $\delta=23$, 67, 547, 661, 1093, 3851, ..., or various numbers composed of these factors.

NOTE ON CERTAIN QUADRATIC NUMBER SYSTEMS FOR WHICH FACTORIZATION IS UNIQUE.

By G. B. BIRKHOFF.

If we define w either as a root of an equation

$$w^2=\frac{D}{4}=0\ldots(1),$$

where D is a negative integer $\equiv 0 \pmod 4$, or as a root of the equation

$$w^2+w+\frac{1-D}{4}=0\ldots(1'),$$

where D is a negative integer $\equiv 1 \pmod 4$, then the set of complex numbers

$$m+nw\ldots(2),$$

m and n real integers, possesses the notable property of being closed under addition and multiplication just as the set of real integers is.

The theorem concerning the uniqueness of the decomposition of real integers into prime factors is based on the algorithm of the greatest common divisor. This algorithm depends on the fact that for all real numbers ξ it is possible to choose a real integer m such that

$$|\xi-m|<1\ldots(3).$$

The complete formal analogy between the complex number system (2) and the set of real integers leads to the remark: If w be such that for all complex numbers ξ it is possible to determine a complex number $m+nw$ such that

$$|\xi-(m+nw)|<1\ldots(4),$$

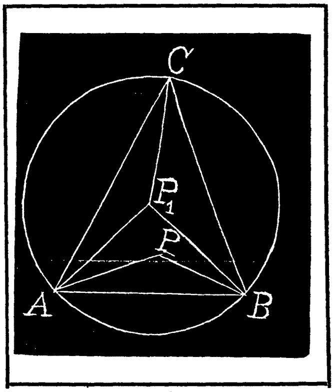
then the theorem of unique decomposition holds for these number systems. It is the purpose of this note to determine, by a geometrical scheme, for which of these systems condition (4) obtains.

In the complex plane we mark off the network of points $m+nw$, in particular the points $A\equiv 0$, $B\equiv 1$, $C\equiv w$. Since the real part of w is either 0 or $\frac{1}{2}$, the projection of C on AB falls on AB, which is of length 1, and *the triangle ABC is an acute or right triangle.* Further we write $w=r.e^{i\theta}$, whence noting that

$$|w|=\sqrt{-\frac{D}{4}} \text{ or } |w| \sqrt{\frac{1-D}{4}},$$

we obtain $\quad r\geqq 1\ldots(5).$

Consider the points Q of the network $m+nw$ and a point P of the plane. At each point P there is clearly a least of the distances PQ; we call this distance $d(P)$. The condition (4) is then equivalent to the condition



$$d(P)<1\ldots(6) \text{ for all points } P.$$

In order to give the condition (5) explicit form we construct the circumcenter P_1 of the triangle ABC, so that

$$P_1A=P_1B=P_1C=\rho\ldots(7);$$

also since this triangle is acute or right, P_1 does not lie without the triangle. We first prove that

$$d(P_1)=\rho\ldots(8).$$

By (7) it is clear that if (8) is not true we have $PQ<\rho$ for some Q not A, B, or C; then Q is within the circumscribing circle. Assume if possible such a point Q to exist. From the character of the network it is clear that Q is not within the triangle ABC and accordingly Q must lie on one of the three circular segments, as AB. If then we imagine the network as made up of the intersection of two families of equidistant parallel lines, parallel to CA and CB, it is clear that the line parallel to CA through Q intersects AB produced from B, in β, and that the line parallel to CB through Q intersects AB, produced from A, in α. Thus

$$\angle\beta Q\alpha\geqq\angle BQA\ldots(9).$$

But $$\angle BQA+\angle ACB>180^\circ\ldots(10),$$

since Q lies in the circle on the opposite side of AB from C. Further it is obvious that $\angle ACB=\angle\beta Q\alpha$. Adding corresponding sides of these equations we infer that, after dividing the inequality by 2, $\angle ACB>90^\circ$, which is not possible as the triangle ABC is an acute or right triangle. Hence (8) is proved.

Consider now an arbitrary point P of the triangle ABC, not P_1; then P lies on one of the triangles AP_1B, BP_1C, CP_1A, say AP_1B, so that $AP+PB<AP_1+P_1B(=2\rho)$. Therefore either AP or $PB<\rho$, whence

$$d(P)<\rho,\ P \text{ not at } P_1\ldots(11).$$

From (8) and (11) we infer that

$$\text{Maximum } d(P)=\rho\ldots(12)$$

for the triangle ABC, and hence for the plane, as the whole plane can be built of such triangles. Thus (6) is equivalent to

$$\rho<1\ldots(13).$$

But $\rho=\dfrac{BC}{2\sin\angle BAC}=\dfrac{\sqrt{(1+r^2-2r\cos\theta)}}{2\sin\theta}$, so that (13) is the same as $1+r^2-2r\cos\theta<2\sin\theta$, or $(r-\cos\theta)^2<3\sin^2\theta$. Noting that from (5), $r\geqq\cos\theta$, we find that

$$r<2\cos(\theta-60^\circ)\ldots(14).$$

This makes $r<2$ so that for systems (1)

$$-\frac{D}{4}=1,\ 2,\ 3,$$

and for systems (1′),

$$\frac{1-D}{4}=1,\ 2,\ 3,$$

are the possible cases. Investigating these cases using (14), we find that (4) obtains for the equations

$$w^2+1=0;\ w^2+2=0;\ w^2+w+1=0;\ w^2+w+2=0;\ w^2+w+3=0\ldots(15).$$

In these cases we have a greatest common divisor process.

If we define a prime number N of a system (1) or (1′) as one which has no factor n such that $1<|n|<|N|$, we have the theorem:

Every number N of one of the systems (15) can be decomposed essentially in but one way into prime factors. The non-essential variations are obtained frem the factors f such that $|f|=1$, which are the complete units.

The work here given completes the consideration of the case for a negative discriminant D, and agrees with the results of Dedekind, *Zahlentheorie*, fourth edition, page 450.

◆

ON THE CHORD OF CONTACT OF TANGENTS TO A CONIC.

By W. D. LAMBERT, Washington, D. C.

If we wish to find the equation of the chord of contact of tangents drawn from a point $P_1\equiv(x_1, y_1)$, to the conic[*]

$$Ax^2+Bxy+Cy^2+Dx+Ey+F=0\ldots(1),$$

the straightforward way is to denote the unknown points of contact $P_2\equiv(x_2, y_2)$ and $P_3\equiv(x_3, y_3)$, and proceed to find the values of those coördinates. For this purpose we get two equations by substituting (x_2, y_2) and (x_3, y_3) in (1), and two more by expressing the fact that P_2 lies on the tangents through P_2 and P_3. These are

$$Ax_1x_2+\frac{B}{2}(x_1y_2+x_2y_1)+Cy_1y_2+\frac{D}{2}(x_1+x_2)+\frac{E}{2}(y_1+y_2)+F=0\ldots(2),$$

---

[*] I carry the work through for the general case, but as beginners are likely to be appalled by the mere length of an equation that is simple enough in principle, it is advisable in teaching to take at first a simpler special form of the equation of the conic.